サイバーフィジカル空間におけるリスク連鎖を考慮した防御分析最適化モデル

サイバーフィジカル空間におけるリスク連鎖を考慮した防御分析最適化モデル

Optimization of Risk Chain-based Defense Analysis Model in Cyber-physical Space

大山慎雄
Yoshio Oyama
指導教員　金井敦

法政大学大学院理工学研究科応用情報工学専攻修士課程

There is a complex relationship between the risk of information leakage and countermeasures in an organization. For information leakage risk, there is a chain of risk events due to the coordination of organizations, and for risk countermeasures, it is difficult to evaluate the effectiveness of countermeasures because the impact of implementation extends to multiple risk events. Therefore, in an environment with many devices, it is difficult to detect incidents and determine the management and monitoring points for incident response, and it is considered problematic that the understanding of risks and the optimization of protective measures are performed empirically. In addition, risk analysis and evaluation are often conducted separately for cyberspace and physical space, which does not necessarily correspond to the reality of intertwining these two areas. In this study, we propose an optimization method for the control analysis model by integrating cyberspace and physical space, representing these risk chains in a state transition diagram, and using an analysis method for our previous model to visualize the results of risk countermeasures. In this paper, we propose an optimization method for the control analysis model based on our previous research model, which is based on the concept of the critical path. We verify and confirm that this method enables us to respond to changes in the risk situation that occur in reality, and to optimize the protection against related risks and to optimize the protection cost based on the concept of the critical path.

***Key Words** : Security model*

１．はじめに

会社などの組織において，情報漏洩は長い期間問題となっている．近年では，内部不正による情報漏洩が情報セキュリティ 10 大脅威に挙げられている[1]．そのため組織では，情報漏洩リスクを低減するために対策を施す必要がある．しかし組織における情報漏洩のリスクやその対策には，情報漏洩リスクに関しては組織が連携していることによるリスク事象の連鎖がありリスク対策に関しては実施の影響が複数のリスク事象に及ぶために対策の効果を評価することが困難であるなど，複雑な関係性があるため，状況を把握することが容易ではない．このため，リスクの把握や防御対策の最適化が経験的に行われ，それにより人によって異なる対策を施してしまう問題がある．さらにサイバー空間と物理空間でも対応が異なるため，リスクを正確に把握することが課題となっている．またサイバー空間と物理空間で対応部署が異なることで，それぞれの対策が独立してしまっている側面もある．

セキュリティリスクを分析する際には，FTA（Fault Tree Analysis）分析や ATA（Attack Tree Analysis）分析を用いて行うのが一般的である．しかしこれらの分析手法は，分析対象や分析事項が多くなるにつれて，FT(Fault Tree)図が肥大化することによる計算量の増加やリスク連鎖の関係を体系的に把握することが困難であることが課題として挙げられる．

加藤らの研究[2]では，複雑なリスク連鎖の関係を体系的に分析する手法が提案されている．しかし加藤らの研究ではサイバー空間に限定して分析を行っており，物理空間については，分析は行われていない．

我々は先行研究[3]において，サイバー空間と物理空間の両空間におけるリスク分析を統合的に行い，状態遷移図モデルで表現することにより，複雑なリスク連鎖の体系的把握を実現する手法を提案した．また，先行研究[3]

では上記手法により得られた状態遷移図のそれぞれの経路に対するリスク値の算出式を定義し，最も脆弱な経路をクリティカルパスと定義した．

本研究では，クリティカルパス上に存在する個別のリスク要因にセキュリティ対策を施すことで，クリティカル全体のリスク値を低減するとともに各経路のリスク値を平準化するセキュリティリスク対策の手法を提案する．具体的には上記手法の検証として，この手順を繰り返し行うことで防御の最適化が防御コストを抑えながら達成できる点について考察を行った．その結果，クリティカルパス上に対策を施すことが最もリスク値を下げることが判明した．

本論文の構成を以下に述べる．まず 2 章で既存研究とその問題点を述べる．その後，3 章で分析を行う上での前提条件を定義し，モデル化を行い，4 章では前提条件に基づきリスク分析を行った後，5 章で評価，考察を行う．最後に 6 章で今後の課題を述べる．

２．既存研究とその問題点

（１）木構造分析によるリスク分析

一般的なセキュリティリスク分析手法として挙げられるのが FTA（Fault Tree Analysis）である．FTA は好ましくない事象からその原因を逐次下位レベルに展開して，頂上事象と呼ばれる最上位事象とその原因の関係を定性的，定量的に把握する目的で用いられる手法である．リスク発生確率を算出するための FTA は頂上事象に発生が好ましくないリスクを置き，対策実施の有無によってリスクが発生する確率が変化すると捉え，対策を基本事象とする[4]．また ATA（Attack Tree Analysis）は FTA に似た構造を取り，脅威となる攻撃を引き起こす他の攻撃や原因などを分析し可視化するために使用されている．これらの分析手法には，具体的な攻撃方法や原因などを把握することで，それらを緩和する手段を発見し，対策が可能になる利点がある．しかし，分析の対象や条件により FTA 図が肥大化することが課題である．さらに，ある FT の一部が別の FT に含まれる FT 重複の問題がある[2]．FT の重複は分析の労力や対策選定のための計算量の点で問題となる．そのため，リスク連鎖の関係を体系的に把握することが困難となる．

（２）共通事象を考慮したリスク計算法

EDC（Event tree and Defense tree Combined method）手法[6]では，イベントツリーとディフェンスツリー分析を併用して職種や規模，脅威となる攻撃を定めて分析を行い，分析結果と制約条件から最適な対策を算出することができる．相原ら[6]の研究では，1 つの攻撃が複数事象に影響を与える共通事象問題を考慮した提案を行っている．しかし木構造による分析であるため，分岐が膨大になる問題は解決できていない．

（３）状態遷移リスクモデル

加藤ら[2]の研究では，サイバー環境においてリスクが顕在化する流れやサービス利用の流れを状態遷移図で表現し，対策と合わせてネットワークモデルへ配置することで，リスク，利便性，対策の関係を視覚的に把握することができるモデルを提案した．しかし，物理環境については扱っていない．

この問題に対して，我々は先行研究[3]において，サイバー環境と物理空間を統合し，これらのリスク連鎖を状態遷移図で表現したうえでリスク対策を実施した結果を可視化するモデルを提案した．本論文ではこのモデルの精緻化と，後述するクリティカルパスの概念に基づき関連リスクに対する防御の最適化ならびに防御コスト最適化を実施した．

３．サイバーフィジカル空間のモデル化，制約条件

（１）ネットワーク環境のモデル化，制約条件

まずネットワーク環境についてモデル化と条件定義を行う．一般的に，組織や企業のネットワークは DMZ，イントラネットなどの領域に分けられると仮定する．また Web サーバ，メールサーバ，ファイルサーバを運用していると想定する．部署ごとにイントラネットを分けられることも考えられるが，本論文では簡単のため行わない．以上の条件により本論文において分析を行うネットワーク構成を図 1 に示す．

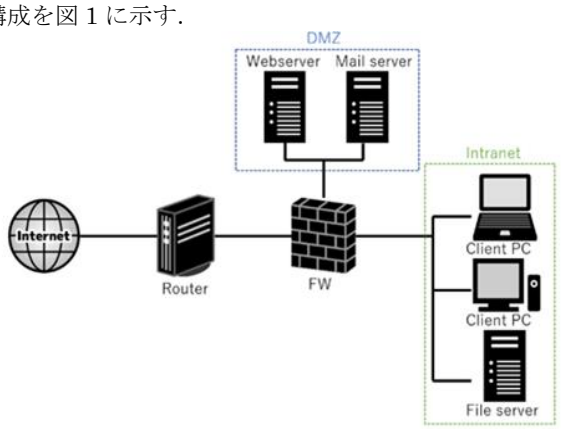

図 1 想定するネットワーク構成

（２）物理空間のモデル化

次に物理環境についてモデル化と条件定義を行う．本論文では一般的に企業には，①企業内部，②一般社員エリア，③重要室が存在すると仮定する．①企業内部への侵入には受付が必要であると仮定する．②一般社員エリアでは覗き見や聞き耳などの脅威が存在すると想定する．また③重要室には個人情報等の情報資産を保有すると仮定する．また，図 2 に示すように，個人情報を保存したときに個人情報漏洩の脅威レベルが最も高いのは，受付を通っただけの①のエリアに保存したときであり，次いで社員証で認証した②のエリア，さらにカードキーで認証した③の順になり，③の重要室に保存することで最も脅

威レベルが低くなると考えられる．

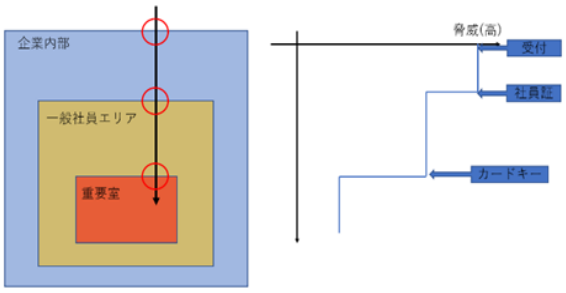

図 2 想定する物理環境モデル

4．サイバーフィジカル空間における情報漏洩リスクモデル作成手法の提案

（1）FTA 分析

本研究では，最初に情報資産の漏洩に関する全体の事象を把握するために，FTA を表 1 の全要因に対して行った．まず，組織の保有する情報資産についての FTA 分析を行う．しかし，FTA 分析を網羅的に行うことは容易ではない．そのため，米田ら[7]の RBS（Risk Breakdown Structure）手法に基づく場のセキュリティにおけるリスク要因抽出結果を参考に，情報漏洩に関する項目を抽出することでこれを解決した．場のセキュリティとは本研究で用いる物理空間のことである．本研究では情報の消失は扱わない．例えば，物理セキュリティにおいて「放火」は例え社屋が全焼しても情報の消失は考えられるが情報の流出はないと仮定する．また，「DoS（Denial of service attack）攻撃」による Web サービスの停止を原因とする情報の消失は考えられるが情報流出は想定しない．以下に示す表 1 に，物理セキュリティとサイバーセキュリティに関するリスク要因をまとめた．情報漏洩は，表 1 のリスク要因として示した要因のうち 1 つでも発生するとインシデントとして現れる．

次に，表 1 に示したリスク要因のうち，「1.1 侵入」について分析した FT 図の一部を図 3 に示す．本論文では図示していないが，「侵入」をはじめとする物理セキュリティとサイバーセキュリティを合わせた 13 件のリスク要因は表 1 を基に上記で説明したように，「情報漏洩」事象下にて OR 端子で結ばれている．言い換えると表 1 の事象のいずれかが起こった時に情報漏洩が発生すると仮定する．図 3 は四角で示した事象を論理演算子で結んだものとなっている．図 2 に示した物理環境モデルにおける情報漏洩インシデントは，図 3 で最上部に配置した「（重要室への）侵入」によって発生する．「（重要室への）侵入」は AND 端子で結んでいる事象「企業内部に侵入」，「一般社員エリアに侵入」，「重要室にアクセス」のすべてが達成されたときに発生する．また図 3 の「一般社員エリアに侵入」という事象の下に OR 端子で結んでいる

表 1 RBS 手法に基づく情報漏洩に関するリスク要因

分類	リスク要因
1.物理セキュリティ	1.1.侵入
	1.2.盗難
	1.3.聞き出し
	1.4.覗き見
	1.5.聞き耳
	1.6.紛失
	1.7.内部犯行
	1.8.書置き
2.サイバーセキュリティ	2.1 ウイルス感染
	2.2 不正アクセス
	2.3 なりすまし
	2.4 フィッシング
	2.5 誤操作

「社員証提示」事象や「共連れ」事象のいずれかの 1 つでも発生すると「一般社員エリアに侵入」事象が達成されることを意味している．

次に，不正アクセスのフォルトツリーを図 4 に示す．図 4 では，物理空間で起こる事象をオレンジ色で表現し，ネットワーク空間で起こる事象を青色で表現している．以降この表現は統一する．図 4 を参照すると，物理空間とネットワーク空間が入り混じった状態であることが分かる．また，同じ FT 事象が現れており，例えば図 3 で用いた「侵入事象」の事象が図 4 にも現れていることが分かる．この冗長性によって FT 図は膨大になってしまう．

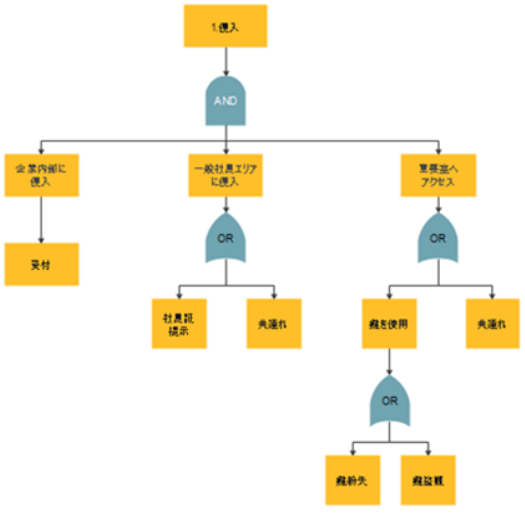

図 3 侵入のフォルトツリーの一部

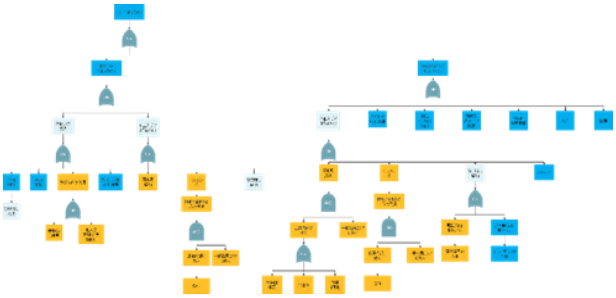

図 4 不正アクセスのフォルトツリーの一部

（２）状態遷移リスクモデル作成手法の提案

4.1 節で作成した FTA 分析に基づき，それぞれの FTA シナリオを対応させるように状態遷移図シナリオを作成する手法を提案する．

図 5 は，表 1 の「侵入」事象のシナリオを状態遷移図によって表記したものである．全体事象に含まれる個別の事象を状態として円形で表記し，遷移時に対策を記載することで次の状態に遷移する確率を表現している．また，図 5 では S1 の「受付」状態や S4 の「一般社員エリアに侵入」，S7 の「重要室にアクセス」のそれぞれの個別事象が複数回使用されていることが確認できる．また状態には全てに番号を振られており，全ての状態は一意に定めることができる．

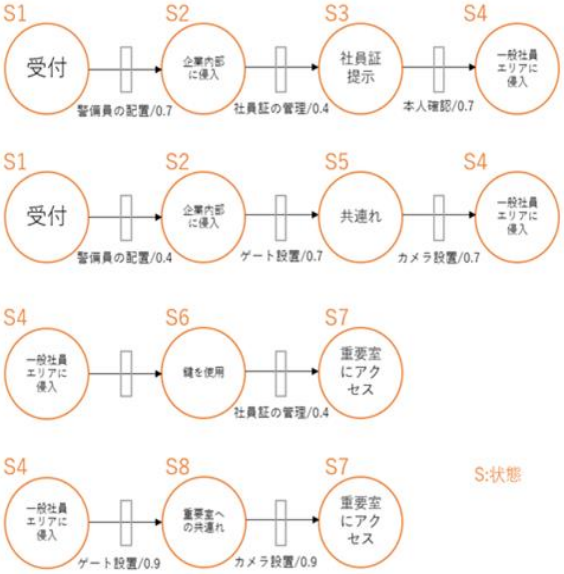

図 5 状態遷移によるリスク表記

（３）状態遷移図の結合

次に 4.2 節で示したような複数回現れる事象を重ね合わせて結合する．この際，状態遷移モデルと FT は対応関係があるため，FT 図下位原因事象が頂上事象に向かって遷移するように，状態遷移の向きに注意する．4.2 節で作成した状態遷移図（図 5）を元に結合を行う．結合時に注意しなければならないのが，個々の状態遷移が前後の状態と無関係， その状態に遷移した原因やその後に続く遷移を検討せずに対策を割り当てるために，状態を細分化して一意になるように定義することが望ましいということである．

しかし，すべての状態遷移が独立となるように分析を行うことは容易ではない．そのため，個々のリスクの分析と結合による不整合の確認を繰り返す中で，妥当なリスク分析結果を得る必要がある．

以上のように，4.1 節 FTA 解析，4.2 節の状態遷移図リスクモデル作成，そして 4.3 節の状態遷移図の結合の手順により，図 7 のようなサイバーフィジカル空間の情報漏洩リスクモデルが作成することができる．なお，本論文では状態遷移図を図示する際に簡略化するため，状態名や対策名は簡易表記としている．また，対策の低減確率を 0，0.4，0.7，0.9 と設定しているが，これは暫定的に設定している．また対策を設定していない項目に関しては「—」で記述している．そして頂上事象である「情報漏洩」事象を赤で表現している．また，モデルに設定した対策を表 2 に示す．表 2 の対策はより優れた対策が発見された場合には現在記されている対策と置き換えることが可能である．そのため対策者は，常に時代に合った最新の対策を適用することが望ましい．

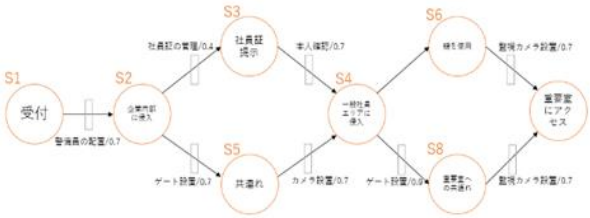

図 6 状態遷移図の結合の一部

５． 評価

（１）事故発生確率，リスク値の算出

図 7 のように作成されたモデルから，情報漏洩リスクを算出する．まず，始点と終点の 2 つの状態を選択する．次に，始点から終点へたどり着くパスを抽出する．これには式(1)を用いて，パス n のリスクP_nを算出する．ここで，パス n に含まれるイベント e とその集合E_n，イベント e の遷移確率や対策による低減確率P_e，対策の実施の有無$x_i \in E\{0,1\}$，対策 i を実施した時のイベント e に対するリスク低減効果を$\Delta P_{e,i}$とする．

$$P_n = \prod_{e \in E_n} P_e \prod_i \left(1 - \Delta P_{e,i} x_i\right) \ldots (1)$$

そして，始点から終点にたどり着く総合的なリスク値P_{total}は，すべてのパスのうち少なくとも 1 つのパスが成立する確率となるため，式(2)により表される．P_{total}の取りうる範囲は 0~1 である．

$$P_{total} = 1 - \prod_{n \in N} (1 - P_n) \ldots (2)$$

サイバーフィジカル空間における情報漏洩リスク分析状態遷移図モデル（図 7）に適用して，式(1)には各経路の開始地点から「情報漏洩」状態までの 2 つの状態を入力

として，式(2)には式(1)より求まったリスク値を入力とすることにより求まったリスク値を表 2，表 3 に示す．表 2 の情報漏洩パスとは漏洩の起点となりうる状態から情報漏洩状態に遷移するまでの経路のことである．本論文では，全 6 つの経路に対して，最大リスクと最小のリスクを算出した．

（2）クリティカルパスの導出による防御対策の検討

一般的に，「クリティカルパス」はプロジェクト上最長の経路を表す．しかし本研究では，リスク値が最大となる情報漏洩パスをクリティカルパスと呼ぶ．表 2 より，「サイト不正アクセス」による情報漏洩パスが 0.07 と最もリスク値が高いことが分かる．これは，「サイト不正アクセス」情報漏洩パスがクリティカルパスであることを示している．つまりこの経路における対策を行うことで，総合リスクを下げることが可能である．図 7 を確認すると，情報漏洩に至るまでの状態数，つまり対策数が少ないことが分かる．そのためサイト不正アクセスの情報漏洩パスにおける状態数を増やすことで，状態遷移時に対策を設定する機会を増やすことができる．つまり，サイト不正アクセスについては，多層防御の概念に基づいた対策が情報漏洩リスクの低減に有効であることが分かる．

（3）クリティカルパスのセキュリティ対策変更による防御の最適化

情報漏洩パスのうちクリティカルパス「サイト不正アクセス」パスが最も脆弱であることを 5.2 節で示し，このクリティカルパス上に対策数を増やすことが有効であることがわかった．そこで本節では，新たな対策をクリティカルパス上に定めることで，防御の最適化を図った．

表 4 を参照し，新しい対策「ID・パスワード変更（リスク低減効果 0.9）」，「ウイルススキャン（リスク低減効果 0.7）」をクリティカルパス上に配置を行い，5.2 節と同様に式(1)，(2)を用いて総合リスクの計算を行った結果を表 5 に示す．この表を参照すると 0.0796 あったリスク値が 0.0124 まで減少していることが分かる．

表 2 情報漏洩リスク値

情報漏洩パス	最大リスク	最小リスク
業務 PC 持ち出し	0.00162	0.00027
業務 PC 盗難	0.00162	0.00027
重要端末持ち出し	0.000486	0.000243
外部メディアによる外部持ち出し	0.0054	0.0027
内部 NW 侵入	0.0012	0.000009
サイト不正アクセス	0.07	0.009

表 3 総合リスク

最大総合リスク	0.0796
最小総合リスク	0.0125

表 4 モデル設定対策案

状態名	対策	低減効果
受付	—	0
企業内部侵入	警備員の配置	0.7
社員証提示	社員証の管理	0.4
一般社員エリアへの共連れ	ゲート設置	0.9
一般社員エリアへの侵入	本人確認 / 監視カメラ設置	0.7 / 0.7
外部メディアに情報保管	外部メディア使用禁止	0.9
鍵を使用	—	0
重要室への共連れ	ゲート設置	0.9
重要室へアクセス	監視カメラ設置	0.7
端末持ち出し	備品の逐次管理	0.7
業務 PC 持ち出し	備品の逐次管理	0.7
業務 PC 盗難	備品の逐次管理	0.7
社員の鍵持ち出し	—	0
鍵盗難	備品の逐次管理	0.7
なりすましによるメール送信	—	0
メール開封	サンドボックス環境下の検証	0.9
Web 閲覧	—	0
ファイル共有サービス使用	セキュリティポリシーによるリスク最小化	0.9
マルウェア感染	セキュリティ対策ソフト	0.9
ID・パスワード入手	ID・パスワードの更新	0.9
入口突破	FW アクセス制御	0.9
内部 NW 侵入	FW アクセス制御	0.9
サイト不正アクセス	FW アクセス制御	0.9
WAF 設定不備	最新パッチの適用	0.9
簡易パスワード設定	簡易パスワード禁止	0.9
SQL インジェクション	WAF 設定 / コード修正	0.9 / 0.7
パスワードリスト攻撃	2 段階認証追加	0.9
トラッシング成功	シュレッダー等の使用	0.7
覗き見成功	覗き見防止シートの活用	0.7

つまり，図 7 に示した情報漏洩リスク状態遷移図に存在する 35 個の状態に対して 2 つの状態を追加するのみで，総合リスクを 0.0672 減少させることに成功した．上記 2 つのセキュリティ対策を追加した後の状態遷移図に対して表 3 の情報漏洩パスそれぞれについて新しく最大リスク値を算出することによりクリティカルパスを導出した．その結果，クリティカルパスは表 6 に示すように対策実施前「サイト不正アクセス」から変化し，「外部メディアによる外部持ち出し」となった．「外部メディアによる外部持ち出し」とは，状態遷移パスである．つまり，より情報漏洩に対するリスク値を下げたい場合，表 6 に示したクリティカルパスの経路に対策を追加することが効率的な情報セキュリティ対策の追加方法であることが示唆される．

対策前は「サイト不正アクセス」と「外部メディアによる外部持ち出し」経路のリスク値の差が 0.0636 であったが，対策後はクリティカルパスの次にリスク値の大きい経路である「サイト不正アクセス」との差は 0.0021 である．対策を行うことにより，経路リスク値の差において 0.0603 減少させることが出来た．

表 5 対策後の総合リスク

	対策前（表 4）	対策後
最大総合リスク	0.0796	0.0124
最小総合リスク	0.0125	0.0038

表 6 対策後の情報漏洩リスク値

情報漏洩パス	最大リスク	最小リスク
業務 PC 持ち出し	0.00162	0.00027
業務 PC 盗難	0.00162	0.00027
重要端末持ち出し	0.000486	0.000243
外部メディアによる外部持ち出し	0.0054	0.0027
内部 NW 侵入	0.0012	0.000009
サイト不正アクセス	0.0021	0.00027

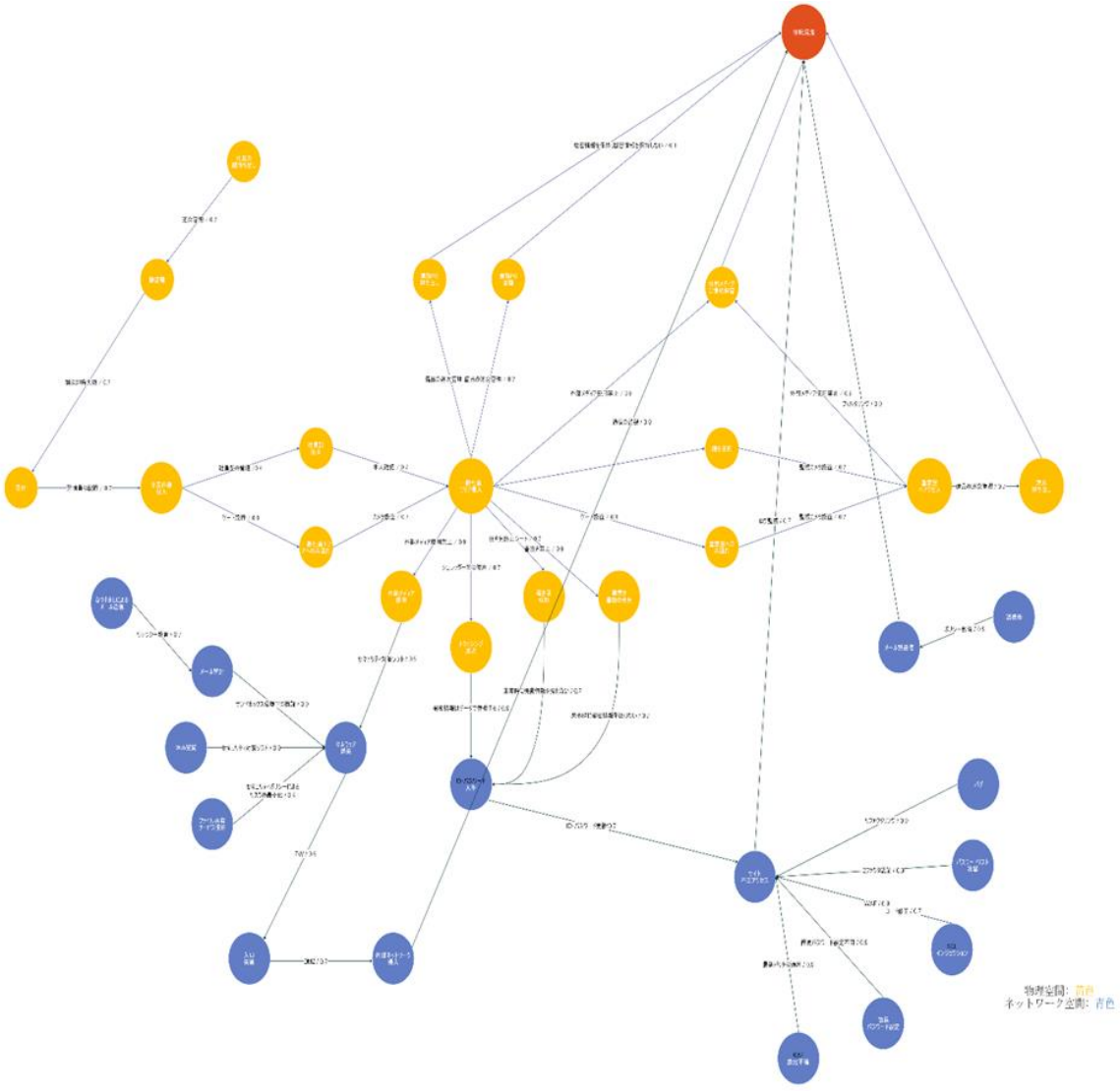

図 7 サイバーフィジカル空間における情報漏洩リスク分析状態遷移図モデル

また，経路ごとのリスク値差は 0.0021 であることから大きなリスク値の差異がないことが確認できる．これにより，現実に発生する情報漏洩リスクに関する状況変化への対応を可能とし，クリティカルパスの概念に基づき関連リスクに対する防御の最適化が可能であることが検証できた．また，上記のことを 2 つの対策のみで実現したことから，防御コストの最適化も行うことが出来たと言える．

６．考察

（１）ペリメータラインの設定

心理面，経済面，物理面に対して定めるセキュリティ防御ライン(ペリメータライン)を効率良く連動させる多層防御の考えを取り入れてモデルを配置することで安心安全なITガバナンスに寄与することが出来ないか検討を行う．

（２）疲労度を考慮した対策設定

本研究では，リスク値のみ着目して分析を行ったが，利用者の疲労度や可用性も考慮した対策を行うことが業務効率化の観点でも望ましい．そのため対策の低減確率だけでなく，ユーザの疲労度測定[8]に基づいた定量的な分析を行うことで可用性も考慮した対策を選択できないか検討を行う．

（３）最適な対策値設定

本研究では，表 4 の通り暫定的に対策の低減確率を定めている．今後の研究では，状態遷移モデルをベイジアンネットワークとして扱い，ベイズ更新[2]を行うことで低減確率を常に最適な対策値に定めることができないか検討を行う．

７．おわりに

本研究では，サイバー空間と物理空間を統合し，これらのリスク連鎖を状態遷移図で表現し，さらにリスク対策を実施した結果を可視化するモデルおよびその分析手法を提案し，リスク値を算出した．これにより現実に発生するリスクの状況変化への対応が可能であることを示し，クリティカルパスの概念に基づいて最適な防御が行うことが可能であることが確認できた．

参考文献

1) IPA：情報セキュリティ 10 大脅威 2020，IPA(オンライン)，入手先 <https://www.ipa.go.jp/security/vuln/10threats2020.html>（参照 2020-10-29）．

2) 加藤弘一， 勅使河原可海：事象連鎖と原因推測が可能なリスク・利便性・対策表示モデルの提案，情報処理学会論文誌，Vol50， No.9， pp219-224，2009

3) 大山慎雄， 金井敦， 谷本茂明， 畑島隆：サイバーフィジカル空間におけるリスク連鎖を考慮した防御分析モデルの提案， 情報処理学会論文誌，Vol50，No.9，pp.219-224，2009

4) 加藤弘一， 勅使河原可海：利便性とセキュリティの動的以降によるユーザ要求の自動交渉方式の検討， 情報処理学会研究報告コンピュータセキュリティ（CSEC），Vol16，No.16，pp.219-224，2007

5) IPA:制御システムのセキュリティ分析ガイド 第 2 版，IPA(オンライン)，入手先 <https://www.ipa.go.jp/security/vuln/10threats2020.html>（参照 2020-10-29）．

6) 相原遼， 佐々木良一：イベントツリーとディフェンスツリーを併用したリスク分析における共通事象を考慮したリスク計算法の提案， マルチメディア，分散，協調とモバイル(DICOMO2016)シンポジウム，Vol2016，No.1，pp.1062-1067，2016

7) 米田翔一，谷本茂明，佐藤周行，金井敦：オフィス空間における場のセキュリティを考慮したリスクアセスメント，情報科学技術フォーラム講演論文集（FIT），Vol2016，No.4，pp.55-58，2014

8) 畑島隆，谷本茂明，金井敦：情報セキュリティ疲労度測定尺度 SFS-9 の開発と信頼性・妥当性，情報処理学会論文誌，Vol.61，No.9，pp1472-1485，2020